路由系列产品流量统计方式经验总结

孟普 2017-06-17 发表

网络问题处理中，工程师经常会碰到网络丢包的问题，网络丢包的原因有很多种，但是排查此类问题的第一步是定位丢包到底是丢在哪一台设备上是因为传输线路的质量问题，只有精准的定位了丢包的位置，才能更快的解决问题，恢复网络的正常。

一、 V5平台的MSR/SR66/SR66-X系列路由器对丢包位置的定位使用包过滤防火墙

1.首先全局开启firewall功能：firewall enable；

2.写两条ACL，分别匹配从10.0.0.1到10.0.0.2与从10.0.0.2到10.0.0.1的icmp报文：

```
acl number 3100
  rule 0 permit icmp source 10.0.0.1 0 destination 10.0.0.2 0
acl number 3200
rule 0 permit icmp source 10.0.0.2 0 destination 10.0.0.1 0
```

3.在G0/0口的出、入方向下应用firewall：

```
firewall packet-filter 3100 outbound
  firewall packet-filter 3200 inbound
```

4.测试前，先清空G0/0接口的防火墙统计信息：

```
reset firewall-statistics interface G0/0
```

5.从SR66路由器ping公网网关10.0.0.2 50个包，然后查看接口统计信息：

```
display firewall-statistics interface g0/0
<SR66>dis firewall-statistics interface GigabitEthernet 0/0
  Interface: GigabitEthernet0/0
  In-bound Policy: acl 3200
  From 2013-12-14 8:14:09 to 2013-12-14 8:17:00
     50 packets, 4200 bytes, 0% permitted,
     0 packets, 0 bytes, 0% denied,
     421438 packets, 84622789 bytes, 100% permitted default,
     0 packets, 0 bytes, 0% denied default,
  Totally 421488 packets, 84626989 bytes, 100% permitted,
  Totally 0 packets, 0 bytes, 0% denied.

  Interface: GigabitEthernet0/0
  Out-bound Policy: acl 3100
  From 2013-12-14 8:14:09 to 2013-12-14 8:17:00
     50 packets, 4200 bytes, 0% permitted,
     0 packets, 0 bytes, 0% denied,
     553218 packets, 585289690 bytes, 100% permitted default,
     0 packets, 0 bytes, 0% denied default,
  Totally 553268 packets, 585293890 bytes, 100% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
```

观察上述信息，会有以下两种现象：

1) Out-bound方向的permit报文为0或者不到50个，则证明报文是在SR66路由器内部丢失的，请排查SR66路由器的配置，以及板间转发信息。

2) Out-bound方向的permit报文为50个，但是In-bound方向为0或者不到50个，则证明SR66路由器并没有收到回应报文，报文在线路或者对端设备丢失，请排查公网线路及设备问题。

二、 V7平台的MSR/SR66系列路由器对丢包位置的定位方法

巧用流量统计判断网络丢包位置：

方法一：

AC上流量统计配置：

```
#
acl number 3001
 rule 0 permit ip source 10.0.0.1 0 destination 10.0.0.2 0
#
traffic classifier 1 operator and //创建类1，匹配规则ACL 3001。
 if-match acl 3001
#
```

通过用户视图下的reset counters interface命令清空流量统计信息。
#
traffic behavior 1 //创建流行为1，流行为为过滤动作允许。AC由于硬件芯片原因暂时不支持流量统计，通过过滤动作允许进行统计。
 filter permit
#
qos policy 1 //创建策略1，指定类1采用流行为1。
 classifier 1 behavior 1
#
interface Ten-GigabitEthernet1/0/1 //接口上应用QoS策略1，并指定应用方向。
 qos apply policy 1 outbound
#
<>display qos policy interface

方法二：
1 首先ACL定义流量的源和目的
 acl advanced 3001
 rule 1 permit icmp source 10.0.0.1 0 destination 10.0.0.2 0 counting/表示使能规则匹配统计功能，缺省为关闭
2 接口下调用packet-filter
 packet-filter 3001 inbound
 packet-filter default inbound hardware-count //用来在接口上使能报文过滤缺省动作统计功能，默认处于关闭状态
 3 清除接口统计信息之后进行PING测试，并且查看接口报文统计信息
清除接口GigabitEthernet0/0入方向上IPv4基本ACL 3001在报文过滤中应用的统计信息。
<Sysname> reset packet-filter statistics interface gigabitethernet 0/0 inbound 3001
进行PING测试
查看入方向的统计信息：
[H3C]display packet-filter statistics interface GigabitEthernet 0/0 inbound
  Interface: GigabitEthernet0/0
  Inbound policy:
  IPv4 ACL 3001
  rule 1 permit ip source 1.0.0.1 0 destination 10.0.0.2 0 counting (5 packets)/可以看到统计到了5个报文，再次PING之后，数量会随之增加。
 IPv4 default action: Permit, Hardware-count
  From 2016-07-01 03:32:49 to 2016-07-01 03:33:32
  Totally 0 packets

三、SR88-X/CR16K/CR16K-F系列路由器对丢包位置的定位方法
使用官网QOS章节用的流量统计方法。

流量统计是快速定位丢包位置最常用的手段，只有定位了丢包的位置，才能精确地进行下一步的排查。